UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,435	09/02/2004	Rene-Michael Cordes	162-110	1274

23117 7590 05/29/2008
NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	PAPER NUMBER
2132	
MAIL DATE	DELIVERY MODE
05/29/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,435	CORDES, RENE-MICHAEL	
	Examiner	Art Unit	
	Samson B. Lemma	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *3-6,14 and 17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/04/2008*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on March 04, 2008. New claims 10-20 are added. Thus claims 1-20 is pending/examined.

Priority

2. Receipt is acknowledged of papers submitted under 35 U.S.C. 119 (a)-(d), which papers have been placed of record in the file.

Response to Arguments

3. Applicant's argument filed on March 04, 2008 have been fully considered and found to be persuasive and a new ground of rejection(s) is made.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1-2, 7-13, 15-16 and 18** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kencheng Zeng** (hereinafter refereed as **Zeng**) (IEEE, Publication title, "Pseudorandom Bit Generators in Stream-Cipher

Cryptography") (Published on 1999) (Submitted with applicant's IDS, with a missing page) (**Note: Complete page of the above reference has been previously attached)** in view of Swindlehurst et al (hereinafter referred as **Swindle**(U.S. Publication No. 2003/0091185) (Published on May 15, 2003)

6. **As per independent claim 1, 11 and dependent claims 10, 12-13, 15-16, 18 Zeng discloses Code generator with a plurality of storage elements ($FF_{1,2,\ldots n}$) connected in a code-producing series (R), e.g., flip-flops**, [See, Figure 6, ref. Num "FF1, FF2, FF3 and FF5 and Page 10, ,middle column, lines 6-14 and figure 5 and See also page 10, middle column up to right hand column line 30], [The elements designated as FF1, FF2, FF3 and FF5 on figure 6 are flip-flops see for the description what is disclosed on page 10, middle column lines 6-14. Furthermore on page 10, middle column, lines 24-30, these flip-flops these are disclosed as storage elements of the FSR called stages, and as shown on figure 6, they are connected in a code-producing series R) **wherein the output of the last storage element (FF_5) in the series (R) is linked with the input of the first storage element (FF_1) in the series (R) to form a circuit,** *[See figure 6, the connection b/n FF_1 and FF_5]* **and outputs and inputs of the storage elements are recursively interconnected with EXOR gates inserted, characterized in that at least one EXOR gate ($EXOR_1$) is provided** *[See, On figure 6, the EX-OR gate],* **whose first input (1) is connected with the output of a storage element (FF_1) located in the code-producing series (R)** *[On figure 6, See ref. "1"],*

whose second input (2) is connected with the output of another storage element (FF_3) located in the code-producing series (R), [On figure 6, see "2"] **and whose output (3) is connected with the input of the storage element (FF_2)** [See figure 6, ref. "3"] **following the storage element (FF_1) connected with the first input (1) of the EXOR gate ($EXOR_{p1}$) in the code-producing series (R),** [See figure 6, "EX-OR gate] and **that the output of a storage element (FF_5) located in the code-producing series (R) is connected with the input of an inverter (INV), and the output of the inverter (INV) is connected with the input of another storage element (FF_1) arranged in the code-producing series (R)** [On figure 6, See Not gate or Inverter], (See also page 10, middle column up to right hand column line 30]. (Note: this is just one way of interpreting the graph, however figure 6 can be interpreted in various ways to meet the above limitation of the claim 1]

Zeng does not explicitly disclose a plurality of EXOR gates instead only shows a single EXOR gate.

However, in the same field of endeavor **Swindle**, on paragraph 0054 and figure 8, discloses the following which meets the above limitation.

"The message byte read from the message register 740 is XORed with one byte from the Sbox memory 78 (sbox_xor_byte) by a plurality of XOR gates 744 and the resulting ciphertext is stored in the cipher register 742. In FIG. 8, the XOR gates 744 each represents plural XOR gates, such as 8 XOR gates."

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features such as a plurality of EXOR gates instead of only a single EXOR gates as per teachings of **Swindle** into the method as taught by **Zeng** in order to provide efficient streaming architecture. [See **Swingle** Abstract]

7. **As per dependent claim 2 Zeng discloses Code generator as applied to claims above. Furthermore, Zeng discloses the code generator**, characterized in that an AND gate (AND.sub.p1) is connected in the line connecting the second input (2) of the at least one EXOR gate (EXOR.sub.p1) and the output of the other storage element (FF.sub.3) located in the code-reproducing series (R), so that the output (4) of the AND gate (AND.sub.p1) is connected with the second input (2) of the EXOR gate (EXOR.sub.p1) the first input (6) of the AND gate (AND.sub.p1) is connected with the output of the other storage element (FF.sub.3) located in the code-producing series (R), and the second input (5) of the AND gate (AND.sub.p1) is connected with the output of a code-programming storage element (FF.sub.p1). **[See at least figure 4]**

8. **As per dependent claims 7-9 Zeng discloses Code generator as applied to claims above. Furthermore, Zeng discloses the code generator**, characterized in that it has at least one connection for at least a second, identically structured code generator, so that both code generators can be supplied with the same program clock at the same time. *[for instance on figure 10, see how the clock is applied, and on page*

14, middle column last paragraph, see at least how the clock is controlled jointly)

9. **Claims 19-20** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kencheng Zeng** (hereinafter refereed as **Zeng**) (IEEE, Publication title, "Pseudorandom Bit Generators in Stream-Cipher Cryptography") (Published on 1999) (Submitted with applicant's IDS, with a missing page) **(Note: Complete page of the above reference has been previously attached)** in view of Shaver (hereinafter referred as **Shaver)** (U.S. Patent No. 5,428,614) (Date of patent Jun 27, 1995)

10. **As per independent claim 19 and dependent claim 20 Zeng discloses Code generator with a plurality of storage elements ($FF_{1,2,...n}$) connected in a code-producing series (R), e.g., flip-flops**, [See, Figure 6, ref. Num "FF1, FF2, FF3 and FF5 and Page 10, ,middle column, lines 6-14 and figure 5 and See also page 10, middle column up to right hand column line 30], [The elements designated as FF1, FF2, FF3 and FF5 on figure 6 are flip-flops see for the description what is disclosed on page 10, middle column lines 6-14. Furthermore on page 10, middle column, lines 24-30, these flip-flops these are disclosed as storage elements of the FSR called stages, and as shown on figure 6, they are connected in a code-producing series R) **wherein the output of the last storage element (FF_5) in the series (R) is linked with the input of the first storage element (FF_1) in the series (R) to form a circuit,** *[See figure 6, the connection b/n FF_1 and FF_5]* **and outputs and inputs of the storage**

elements are recursively interconnected with EXOR gates inserted, characterized in that at least one EXOR gate ($EXOR_1$) is provided *[See, On figure 6, the EX-OR gate],* **whose first input (1) is connected with the output of a storage element (FF_1) located in the code-producing series (R)** *[On figure 6, See ref. "1"],* **whose second input (2) is connected with the output of another storage element (FF_3) located in the code-producing series (R),** [On figure 6, see "2"] **and whose output (3) is connected with the input of the storage element (FF_2)** [See figure 6, ref. "3"] **following the storage element (FF_1) connected with the first input (1) of the EXOR gate ($EXOR_{p1}$) in the code-producing series (R),** [See figure 6, "EX-OR gate] and **that the output of a storage element (FF_5) located in the code-producing series (R) is connected with the input of an inverter (INV), and the output of the inverter (INV) is connected with the input of another storage element (FF_1) arranged in the code-producing series (R)** [On figure 6, See Not gate or Inverter], (See also page 10, middle column up to right hand column line 30]. (Note: this is just one way of interpreting the graph, however figure 6 can be interpreted in various ways to meet the above limitation of the claim 1]

Zeng does not explicitly disclose

two or more logic gates, the logic gates including an EXOR and an EXNOR gate each of which includes first and second inputs respectively coupled to outputs of first and second corresponding storage elements

and an output coupled to an input of a third corresponding storage element.

However, in the same field of endeavor **Shaver**, on paragraph column 4, lines 60-68, discloses the following which meets the above limitation.

"FIG. 4 illustrates a framing apparatus/circuit 26 according to the present invention that relies, in part, on the detection of these twenty expected data bits in the received data stream as an aid to framing. Framer 26 includes a 281-bit shift register 28, leading and trailing flag detect circuits 30, 32, a Hamming code generator circuit 34, ***a 10-bit memory 36,*** *a six-bit memory 38, an expected data detector circuit 40, a decision logic circuit 42, and* ***a plurality of 2-input XOR and XNOR gates 44, 45."***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ the circuit arrangement such as ***a plurality of 2-input XOR and XNOR gates 44, 45" as*** per teachings of **Shaver**, into the method as taught by **Zeng** in order to provide a code generator with minimum error when data stream are decoded. [See **Shaver column 1, lines 6-10 and column 2, lines 13-14**]

Allowable Subject Matter

11. **Claims 3-6, 14 and 17** are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-873-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

05/15/2008

/Samson B Lemma/

Examiner, Art Unit 2132

/Gilberto Barron Jr/

Supervisory Patent Examiner, Art Unit 2132